The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

The vulnerabilities are based on the CVE vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
Algorithmic Research -- PrivateWire Gateway	Buffer overflow in the Online Registration Facility for Algorithmic Research PrivateWire VPN software up to 3.7 allows remote attackers to execute arbitrary code via a long GET request.	2005-12-19 2006-06-27	7.0	CVE-2006-3252 BUGTRAQ BID FRSIRT SECTRACK SECUNIA XF
Apple -- Mac OS X Server Apple -- Mac OS X	Stack-based buffer overflow ImageIO in Apple Mac OS X 10.4 up to 10.4.6 allows attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted TIFF image.	unknown 2006-06-27	7.0	CVE-2006-1469 APPLE FRSIRT BID SECTRACK
cairohost -- VBZooM	Multiple SQL injection vulnerabilities in VBZooM 1.00 and earlier allow remote attackers to execute arbitrary SQL commands via the (1) MemberID parameter to rank.php, and the (2) QuranID parameter to lng.php.	unknown 2006-06-27	7.0	CVE-2006-3238 BUGTRAQ BUGTRAQ BID FRSIRT SECUNIA XF

cairohost -- VBZoom	SQL injection vulnerability in message.php in VBZooM 1.11 and earlier allows remote attackers to execute arbitrary SQL commands via the UserID parameter.	unknown 2006-06-27	7.0	CVE-2006-3239 BUGTRAQ BID XF
CBSMS -- Mambo Module	PHP remote file inclusion vulnerability in mod_cbsms.php in CBSMS Mambo Module 1.0 and earlier, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the mosC_a_path parameter. NOTE: the provenance of this information is unknown; portions of the details are obtained from third party information.	unknown 2006-06-28	7.0	CVE-2006-3302 FRSIRT XF
Cisco -- Secure Access Control Server	Cisco Secure Access Control Server (ACS) 4.x for Windows uses the client's IP address and the server's port number to grant access to an HTTP server port for an administration session, which allows remote attackers to bypass authentication via various methods, aka "ACS Weak Session Management Vulnerability."	unknown 2006-06-26	7.0	CVE-2006-3226 BUGTRAQ BUGTRAQ CISCO BID SECTRACK XF FRSIRT SECUNIA
Cisco -- Wireless Control System	The internal database in Cisco Wireless Control System (WCS) for Linux and Windows before 3.2(51) uses an undocumented, hard-coded username and password, which allows remote authenticated users to read, and possibly modify, sensitive configuration data (aka bugs CSCsd15955).	unknown 2006-06-28	7.0	CVE-2006-3285 CISCO BID FRSIRT SECTRACK SECUNIA XF
Cisco -- Wireless Control System	The internal database in Cisco Wireless Control System (WCS) for Linux and Windows before 3.2(63) stores a hard-coded username and password in plaintext within unspecified files, which allows remote authenticated users to access the database (aka bug CSCsd15951).	unknown 2006-06-28	7.0	CVE-2006-3286 CISCO BID FRSIRT SECTRACK SECUNIA
Cisco -- Wireless Control System	Cisco Wireless Control System (WCS) for Linux and Windows 4.0(1) and earlier uses a default administrator username "root" and password "public," which allows remote attackers to gain access (aka bug CSCse21391).	unknown 2006-06-28	7.0	CVE-2006-3287 CISCO BID FRSIRT SECTRACK SECUNIA XF
Cisco -- IOS	The web interface on Cisco IOS 12.3(8)JA and 12.3(8)JA1, as used on the Cisco Wireless Access Point and Wireless Bridge, reconfigures itself when it is changed to use the "Local User List Only (Individual	unknown 2006-06-28	7.0	CVE-2006-3291 CISCO BID FRSIRT CERT-VN

	Passwords)" setting, which removes all security and password configurations and allows remote attackers to access the system.			SECTRACK SECUNIA XF
Clearswift -- MAILsweeper for SMTP Clearswift -- MAILsweeper for Exchange	Clearswift MAILsweeper for SMTP before 4.3.20 and MAILsweeper for Exchange before 4.3.20 allows remote attackers to bypass the "text analysis", possibly bypassing SPAM and other filters, by sending an e-mail specifying a non-existent or unrecognized character set.	unknown 2006-06-23	7.0	CVE-2006-3215 MIMESWEEPER BID FRSIRT SECUNIA
Codewalkers -- PHP Event Calendar Codewalkers -- ltwCalendar	SQL injection vulnerability in calendar.php in Codewalkers PHP Event Calendar 4.2 allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2006-06-27	7.0	CVE-2006-3248 BUGTRAQ OTHER-REF BID SECTRACK XF
Computer Associates -- Integrated Threat Management Computer Associates -- eTrust PestPatrol Computer Associates -- eTrust Antivirus	Format string vulnerability in CA Integrated Threat Management (ITM), eTrust Antivirus (eAV), and eTrust PestPatrol (ePP) r8 allows attackers to cause a denial of service (crash) and possibly execute arbitrary code via a scan job with format strings in the description field.	2006-06-26 2006-06-27	7.0	CVE-2006-3223 COMPUTER ASSOCIATES OSVDB FULLDISC BUGTRAQ BUGTRAQ BID FRSIRT SECTRACK SECUNIA
datetopia -- Dating Agent PRO	SQL injection vulnerability in Dating Agent PRO 4.7.1 allows remote attackers to execute arbitrary SQL commands via the (1) pid parameter in picture.php, (2) mid parameter in mem.php, and the (3) sex and (4) relationship parameters in search.php.	2006-06-22 2006-06-28	7.0	CVE-2006-3283 BUGTRAQ XF
DeluxeBB -- DeluxeBB	SQL injection vulnerability in cp.php in DeluxeBB 1.07 and earlier allows remote attackers to execute arbitrary SQL commands via the xmsn parameter.	unknown 2006-06-28	7.0	CVE-2006-3304 OTHER-REF BID FRSIRT SECTRACK SECUNIA BUGTRAQ
George Currums -- Open Guestbook	SQL injection vulnerability in view.php in Open Guestbook 0.5 allows remote attackers to execute arbitrary SQL commands via the offset parameter.	unknown 2006-06-28	7.0	CVE-2006-3296 BUGTRAQ BID XF
GraceNote -- CDDBControl ActiveX Control	Buffer overflow in GraceNote CDDBControl ActiveX Control, as used by multiple products that use Gracenote CDDB, allows	2006-04-03 2006-06-27	7.0	CVE-2006-3134 OTHER-REF FULLDISC

	remote attackers to execute arbitrary code via a long option string.			OTHER-REF OTHER-REF CERT-VN BID FRSIRT FRSIRT SECTRACK SECUNIA SECUNIA XF
Hashcash -- Hashcash	Heap-based buffer overflow in the array_push function in hashcash.c for Hashcash before 1.22 might allow attackers to execute arbitrary code via crafted entries.	unknown 2006-06-27	7.0	CVE-2006-3251 OTHER-REF GENTOO BID FRSIRT SECUNIA SECUNIA
IBM -- Websphere Application Server	Unspecified vulnerability in IBM WebSphere Application Server before 6.0.2.11 has unknown impact and attack vectors because the "UserNameToken cache was improperly used."	unknown 2006-06-27	7.0	CVE-2006-3232 OTHER-REF BID FRSIRT SECUNIA
Infinite Core Technologies -- ICT	SQL injection vulnerability in index.php in Infinite Core Technologies (ICT) 1.0 Gold and earlier allows remote attackers to execute arbitrary SQL commands via the post parameter.	unknown 2006-06-27	7.0	CVE-2006-3267 OTHER-REF BID FRSIRT SECUNIA
Internet Scout Project -- Scout Portal Toolkit	SQL injection vulnerability in SPT--ForumTopics.php in Scout Portal Toolkit (SPT) 1.4.0 and earlier allows remote attackers to execute arbitrary SQL commands via the forumid parameter.	unknown 2006-06-28	7.0	CVE-2006-3309 OTHER-REF BID FRSIRT SECUNIA XF
Jaws -- Jaws	SQL injection vulnerability in the Search gadget in Jaws 0.6.2 allows remote attackers to execute arbitrary SQL commands via queries with the "LIKE" keyword in the searchdata parameter (search field).	unknown 2006-06-28	7.0	CVE-2006-3292 BUGTRAQ OTHER-REF OTHER-REF BID FRSIRT SECUNIA XF
LookNet -- FineShop	Multiple SQL injection vulnerabilities in index.php in FineShop 3.0 and earlier allow remote attackers to execute arbitrary SQL commands via the (1) produkt, (2) id_produc, and (3) id_kat parameters.	unknown 2006-06-27	7.0	CVE-2006-3234 OTHER-REF SECTRACK XF

Mambo -- Mambo	SQL injection vulnerability in the Weblinks module (weblinks.php) in Mambo 4.6rc1 and earlier allows remote attackers to execute arbitrary SQL commands via the title parameter.	unknown 2006-06-27	7.0	CVE-2006-3262 BUGTRAQ OTHER-REF OTHER-REF FRSIRT SECTRACK SECUNIA
Mambo -- Mambo	SQL injection vulnerability in the Weblinks module (weblinks.php) in Mambo 4.6rc1 and earlier allows remote attackers to execute arbitrary SQL commands via the catid parameter.	unknown 2006-06-27	7.0	CVE-2006-3263 OTHER-REF
Microsoft -- Windows XP	** DISPUTED ** The Task scheduler (at.exe) on Microsoft Windows XP spawns each scheduled process with SYSTEM permissions, which allows local users to gain privileges. NOTE: this issue has been disputed by third parties, who state that the Task scheduler is limited to the Administrators group by default upon installation.	unknown 2006-06-23	7.0	CVE-2006-3209 BUGTRAQ BUGTRAQ
Microsoft -- Internet Explorer	Cross-domain vulnerability in Microsoft Internet Explorer 6.0 allows remote attackers to access restricted information from other domains via an object tag with a data parameter that references a link on the attacker's originating site that specifies a Location HTTP header that references the target site, which then makes that content available through the outerHTML attribute of the object.	unknown 2006-06-28	7.0	CVE-2006-3280 FULLDISC OTHER-REF BID FRSIRT SECUNIA CERT-VN SECTRACK XF
Mutt -- Mutt	Stack-based buffer overflow in the browse_get_namespace function in imap/browse.c of Mutt 1.4.2.1 and earlier allows remote attackers to cause a denial of service (crash) or execute arbitrary code via long namespaces received from the IMAP server.	unknown 2006-06-27	7.0	CVE-2006-3242 OTHER-REF OTHER-REF BID FRSIRT SECUNIA UBUNTU GENTOO MANDRIVA SECUNIA SECUNIA SECUNIA XF
MyBB -- MyBB	SQL injection vulnerability in usercp.php in MyBB (MyBulletinBoard) 1.0 through 1.1.3 allows remote attackers to execute arbitrary SQL commands via the showcodebuttons	unknown 2006-06-27	7.0	CVE-2006-3243 BUGTRAQ OTHER-REF OTHER-REF

	parameter.			FRSIRT SECUNIA XF
Phorum -- Phorum	SQL injection vulnerability in search.php in Phorum 5.1.14 and earlier allows remote attackers to execute arbitrary SQL commands via the page parameter.	unknown 2006-06-27	7.0	CVE-2006-3249 OTHER-REF
PhpMySms -- PhpMySms	PHP remote file inclusion vulnerability in sms_config/gateway.php in PhpMySms 2.0 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the ROOT_PATH parameter.	unknown 2006-06-28	7.0	CVE-2006-3300 OTHER-REF BID XF
RahnemaCo -- RahnemaCo	PHP remote file inclusion vulnerability in page.php in an unspecified RahnemaCo.com product, possibly eShop, allows remote attackers to execute arbitrary PHP code via a URL in the pageid parameter.	unknown 2006-06-29	7.0	CVE-2006-3314 BUGTRAQ BID SECTRACK
RealNetworks -- Helix DNA Server	Heap-based buffer overflow in RealNetworks Helix DNA Server 10.0 and 11.0 allows remote attackers to execute arbitrary code via (1) a long User-Agent HTTP header in the RTSP service and (2) unspecified vectors involving the "parsing of HTTP URL schemes".	unknown 2006-06-28	7.0	CVE-2006-3276 OTHER-REF BID FRSIRT SECTRACK SECUNIA XF XF
Softbiz -- Dating Script	Multiple SQL injection vulnerabilities in Softbiz Dating 1.0 allow remote attackers to execute SQL commands via the (1) country and (2) sort_by parameters in (a) search_results.php; (3) browse parameter in (b) featured_photos.php; (4) cid parameter in (c) products.php, (d) index.php, and (e) news_desc.php.	unknown 2006-06-28	7.0	CVE-2006-3271 BUGTRAQ BID FRSIRT SECUNIA
Softnews Media Group -- DataLife Engine	SQL injection vulnerability in index.php in DataLife Engine 4.1 and earlier allows remote attackers to execute arbitrary SQL commands via double-encoded values in the user parameter in a userinfo subaction.	2006-06-21 2006-06-24	7.0	CVE-2006-3221 Milw0rm Milw0rm BID FRSIRT SECUNIA XF
thinkfactory -- thinkWMS	Multiple SQL injection vulnerabilities in thinkWMS 1.0 and earlier allow remote attackers to execute arbitrary SQL commands via the (1) id parameter in (a) index.php or (b) printarticle.php, and the (2) catid parameter in index.php.	unknown 2006-06-27	7.0	CVE-2006-3236 OTHER-REF BID FRSIRT SECTRACK SECUNIA XF

THoRCMS -- THoRCMS	SQL injection vulnerability in cms_admin.php in THoRCMS 1.3.1 allows remote attackers to execute arbitrary SQL commands via multiple unspecified parameters, such as the add_link_mid parameter. NOTE: the provenance of this information is unknown; portions of the details are obtained from third party information.	unknown 2006-06-28	7.0	CVE-2006-3270 FRSIRT
WeBBoA -- WeBBoA	SQL injection vulnerability in WeBBoA Hosting 1.1 allows remote attackers to execute arbitrary SQL commands via the id parameter to an unspecified script, possibly host/yeni_host.asp.	unknown 2006-06-23	7.0	CVE-2006-3213 BUGTRAQ BID FRSIRT SECTRACK XF
Woltlab -- Burning Board	SQL injection vulnerability in profile.php in Woltlab Burning Board (WBB) 2.1.6 allows remote attackers to execute arbitrary SQL commands via the userid parameter.	unknown 2006-06-24	7.0	CVE-2006-3218 BUGTRAQ
Woltlab -- Burning Board	SQL injection vulnerability in thread.php in Woltlab Burning Board (WBB) 2.2.2 allows remote attackers to execute arbitrary SQL commands via the threadid parameter.	unknown 2006-06-24	7.0	CVE-2006-3219 BUGTRAQ
Woltlab -- Burning Board	SQL injection vulnerability in studienplatztausch.php in Woltlab Burning Board (WBB) 2.2.1 allows remote attackers to execute arbitrary SQL commands via the sid parameter.	unknown 2006-06-24	7.0	CVE-2006-3220 BUGTRAQ XF
Woltlab -- Burning Board	SQL injection vulnerability in newthread.php in Woltlab Burning Board (WBB) 2.0 RC2 allows remote attackers to execute arbitrary SQL commands via the boardid parameter.	unknown 2006-06-27	7.0	CVE-2006-3254 BUGTRAQ BID SECTRACK
Woltlab -- Burning Board	SQL injection vulnerability in showmods.php in Woltlab Burning Board (WBB) 1.2 allows remote attackers to execute arbitrary SQL commands via the boardid parameter.	unknown 2006-06-27	7.0	CVE-2006-3255 BUGTRAQ BID SECTRACK
Woltlab -- Burning Board	SQL injection vulnerability in report.php in Woltlab Burning Board (WBB) 2.3.1 allows remote attackers to execute arbitrary SQL commands via the postid parameter.	unknown 2006-06-27	7.0	CVE-2006-3256 BUGTRAQ BID SECTRACK
YaBB -- YaBB SE	SQL injection vulnerability in profile.php in YaBB SE 1.5.5 and earlier allows remote attackers to execute SQL commands via a double-encoded user parameter in a viewprofile action.	2006-06-26 2006-06-28	7.0	CVE-2006-3275 FULLDISC BID FRSIRT SECUNIA XF

Zoid Technologies -- Project Eros bbsengine	Multiple SQL injection vulnerabilities in Project EROS bbsengine before bbsengine-20060429-1550-jam allow remote attackers to execute arbitrary SQL commands via (1) unspecified parameters in the php/comment.php and (2) the getpartialmatches method in php/aolbonics.php.	unknown 2006-06-28	7.0	CVE-2006-3307 OTHER-REF BID FRSIRT SECUNIA XF
Zoid Technologies -- Project Eros bbsengine	Unspecified vulnerability in the wpprop code for Project EROS bbsengine before 20060622-0315 has unknown impact and remote attack vectors via [img] tags, possibly cross-site scripting (XSS).	unknown 2006-06-28	7.0	CVE-2006-3308 OTHER-REF BID FRSIRT SECUNIA

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
AEwebworks Dating Software -- aeDating	Cross-site scripting (XSS) vulnerability in aeDating 4.1 allows remote attackers to inject arbitrary web script or HTML via the (1) Sex parameter in index.php, (2) ProfileType parameter in join_form.php, and (3) Email parameter in forgot.php.	2006-06-22 2006-06-28	4.7	CVE-2006-3279 BUGTRAQ FRSIRT SECUNIA XF
Anthill -- Anthill	Multiple SQL injection vulnerabilities in Anthill 0.2.6 and earlier allow remote attackers to execute arbitrary SQL commands via the (1) order parameter in buglist.php and the (2) bug parameter in query.php.	unknown 2006-06-27	5.6	CVE-2006-3244 OTHER-REF SECUNIA BID FRSIRT XF
Apple -- Mac OS X Server Apple -- Mac OS X	Format string vulnerability in the CF_syslog function launchd in Apple Mac OS X 10.4 up to 10.4.6 allows local users to execute arbitrary code via format string specifiers that are not properly handled in a syslog call in the logging facility, as demonstrated by using a crafted plist file.	unknown 2006-06-27	4.9	CVE-2006-1471 APPLE FRSIRT BUGTRAQ BID SECTRACK
CBSMS -- Mambo Module	PHP remote file inclusion vulnerability in mod_cbsms_messages.php in CBSMS Mambo Module 1.0 and earlier, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the mosConfig_absolute_path parameter.	2006-06-26 2006-06-28	5.6	CVE-2006-3294 OTHER-REF BID FRSIRT SECUNIA XF
DeluxeBB -- DeluxeBB	Multiple cross-site scripting (XSS) vulnerabilities in pm.php in DeluxeBB 1.07 and earlier allow remote attackers to inject	unknown 2006-06-28	4.7	CVE-2006-3303 OTHER-REF FRSIRT

	arbitrary web script or HTML via the (1) subject or (2) to parameters.			SECTRACK SECUNIA XF
Jochen Friedrich -- pinball	Unspecified vulnerability in pinball 0.3.1 allows local users to gain privileges via unknown attack vectors that cause pinball to load plugins from an attacker-controlled directory while operating at raised privileges.	unknown 2006-06-26	4.9	CVE-2006-2196 DEBIAN FRSIRT SECUNIA SECUNIA XF
Le R'alf -- Ralf Image Gallery	Ralf Image Gallery (RIG) 0.7.4 and earlier, when register_globals is enabled, allows remote attackers to conduct PHP remote file inclusion and directory traversal attacks via URLs or ".." sequences in the (1) dir_abs_src parameter in (a) check_entry.php, (b) admin_album.php, (c) admin_image.php, and (d) admin_util.php; and the (2) dir_abs_admin_src parameter in admin_album.php and admin_image.php. NOTE: this issue can be leveraged to conduct cross-site scripting (XSS) attacks.	2006-06-12 2006-06-23	5.6	CVE-2006-3210 BUGTRAQ OTHER-REF FRSIRT SECUNIA
MagNet -- Bee-hive Lite	Multiple PHP remote file inclusion vulnerabilities in Bee-hive Lite 1.2 and earlier, when register_globals is enabled, allow remote attackers to execute arbitrary PHP code via a URL in the (1) header parameter to (a) conad/include/rootGui.inc.php and (b) include/rootGui.inc.php; (2) mysqlCall parameter to (c) conad/changeEmail.inc.php, (d) conad/changeUserDetails.inc.php, (e) conad/checkPasswd.inc.php, (f) conad/login.inc.php and (g) conad/logout.inc.php; (3) mysqlcall parameter to (h) include/listall.inc.php; (4) prefix parameter to (i) show/index.php; and (5) config parameter to (j) conad/include/mysqlCall.inc.php.	unknown 2006-06-27	5.6	CVE-2006-3266 OTHER-REF FRSIRT SECUNIA
Microsoft -- Windows Live Messenger	Heap-based buffer overflow in Windows Live Messenger 8.0 allows user-complicit attackers to execute arbitrary code via a crafted Contact List (.ctt) file, which triggers the overflow when it is imported by the user.	unknown 2006-06-27	5.6	CVE-2006-3250 OTHER-REF BID SECTRACK BUGTRAQ OTHER-REF XF
Microsoft -- Internet Explorer	Microsoft Internet Explorer 6.0 allows remote user-complicit attackers to execute arbitrary code via a link to an SMB file share with a filename that contains encoded ..\	unknown 2006-06-28	5.6	CVE-2006-3281 FULLDISC OTHER-REF BID

	(%2e%2e%5c) sequences and whose extension contains the CLSID Key identifier for HTML Applications (HTA). NOTE: this could be a directory traversal vulnerability, although its role in the exploit was not explained. NOTE: this issue might be in other components that are used by Internet Explorer.			FRSIRT SECUNIA CERT-VN SECTRACK XF
MiMMS -- mimms	Stack-based buffer overflow in MiMMS 0.0.9 allows remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via the (1) send_command, (2) string_utf16, (3) get_data, and (4) get_media_packet functions, and possibly other functions.	unknown 2006-06-27	5.6	CVE-2006-2200 OTHER-REF BID FRSIRT SECUNIA
PHP -- PHP	The error_log function in PHP 5.1.4 and 4.4.2 allows local users to bypass safe mode and open_basedir restrictions via a "php://" or other scheme in the third argument, which disables safe mode.	unknown 2006-06-26	4.9	CVE-2006-3011 OTHER-REF FRSIRT SECUNIA BUGTRAQ SECTRACK XF
THoRCMS -- THoRCMS	PHP remote file inclusion vulnerability in includes/functions_cms.php in THoRCMS 1.3.1 allows remote attackers to execute arbitrary PHP code via the phpbb_root_path parameter.	unknown 2006-06-28	5.6	CVE-2006-3269 OTHER-REF BID FRSIRT SECUNIA
Ultimate PHP Board -- Ultimate PHP Board	Direct static code injection vulnerability in Ultimate PHP Board (UPB) 1.9.6 and earlier allows remote authenticated administrators to execute arbitrary PHP code via multiple unspecified "configuration fields" in (1) admin_chatconfig.php, (2) admin_configcss.php, (3) admin_config.php, or (4) admin_config2.php, which are stored as configuration settings. NOTE: this issue can be exploited by remote attackers by leveraging other vulnerabilities in UPB.	unknown 2006-06-23	4.2	CVE-2006-3208 BUGTRAQ OTHER-REF

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
Apple -- Mac OS X	Unspecified vulnerability in Apple File Protocol (AFP) server in Apple Mac OS X 10.4 up to 10.4.6 includes the names of restricted files and folders within search	unknown 2006-06-27	2.3	CVE-2006-1468 APPLE FRSIRT BID

	results, which might allow remote attackers to obtain sensitive information.			BID SECTRACK
Apple -- Mac OS X Server Apple -- Mac OS X	OpenLDAP Apple Mac OS X 10.4 up to 10.4.6 allows remote attackers to cause a denial of service (crash) via an invalid LDAP request that triggers an assert error.	unknown 2006-06-27	2.3	CVE-2006-1470 APPLE FRSIRT CERT-VN BID BID SECTRACK
Apple -- Safari	Apple Safari 2.0.3 (417.9.3) on Mac OS X 10.4.6 allows remote attackers to cause a denial of service (CPU consumption) via Javascript with an infinite for loop. NOTE: it could be argued that this is not a vulnerability, unless it interferes with the operation of the system outside of the scope of Safari itself.	unknown 2006-06-26	2.7	CVE-2006-3224 FULLDISC XF
Azureus Tracker -- Azureus Tracker	Cross-site scripting (XSS) vulnerability in index.tmpl in Azureus Tracker 2.4.0.2 and earlier (Java BitTorrent Client Tracker) allows remote attackers to inject arbitrary web script or HTML via the search parameter.	unknown 2006-06-27	1.9	CVE-2006-3230 OTHER-REF FRSIRT SECUNIA SECTRACK
BNBT -- TrinEdit BNBT -- EasyTracker	Multiple cross-site scripting (XSS) vulnerabilities in index.html in BNBT TrinEdit and EasyTracker 7.7r3.2004.10.27 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) filter or (2) sort parameters.	unknown 2006-06-27	1.9	CVE-2006-3258 BLOGSPOT SECUNIA FRSIRT SECTRACK
Cisco -- Wireless Control System	Unspecified vulnerability in the TFTP server in Cisco Wireless Control System (WCS) for Linux and Windows before 3.2(51), when configured to use a directory path name that contains a space character, allows remote authenticated users to read and overwrite arbitrary files via unspecified vectors.	unknown 2006-06-28	2.3	CVE-2006-3288 CISCO BID FRSIRT SECTRACK SECUNIA XF
Cisco -- Wireless Control System	Cross-site scripting (XSS) vulnerability in the login page of the HTTP interface for the Cisco Wireless Control System (WCS) for Linux and Windows before 3.2(51) allows remote attackers to inject arbitrary web script or HTML via unspecified vectors involving a "malicious URL".	unknown 2006-06-28	1.9	CVE-2006-3289 CISCO BID FRSIRT SECTRACK SECUNIA XF
Cisco -- Wireless Control System	HTTP server in Cisco Wireless Control System (WCS) for Linux and Windows before 3.2(51) stores sensitive information under the web root with insufficient access	unknown 2006-06-28	2.3	CVE-2006-3290 CISCO BID FRSIRT

	control, which allows remote attackers to obtain usernames and directory paths via a direct URL request.			SECTRACK SECUNIA XF
cjGuestbook -- cjGuestbook	Cross-site scripting (XSS) vulnerability in sign.php in cjGuestbook 1.3 and earlier allows remote attackers to inject Javascript code via a javascript URI in an img bbcode tag in the comments parameter.	unknown 2006-06-23	2.3	CVE-2006-3211 BUGTRAQ FRSIRT SECUNIA BID XF
cjGuestbook -- cjGuestbook	Cross-site scripting (XSS) vulnerability in sign.php in cjGuestbook 1.3 and earlier allows remote attackers to inject web script or HTML via the (1) name, (2) email, (3) add, and (4) wName parameters. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2006-06-23	2.3	CVE-2006-3212 BID FRSIRT SECUNIA XF
Claroline -- Claroline	Multiple cross-site scripting (XSS) vulnerabilities in Claroline 1.7.7 allow remote attackers to inject arbitrary HTML or web script via unspecified attack vectors, possibly including (1) calendar/myagenda.php, (2) document/document.php, (3) phpbb/newtopic.php, (4) tracking/userLog.php, and (5) wiki/page.php.	unknown 2006-06-27	2.3	CVE-2006-3257 BUGTRAQ OTHER-REF
Clearswift -- MAILsweeper for SMTP Clearswift -- MAILsweeper for Exchange	Clearswift MAILsweeper for SMTP before 4.3.20 and MAILsweeper for Exchange before 4.3.20 allows remote attackers to cause a denial of service via (1) non-ASCII characters in a reverse DNS lookup result from a Received header, which leads to a Receiver service stop, and (2) unspecified vectors involving malformed messages, which causes "unpredictable behavior" that prevents the Security service from processing more messages.	unknown 2006-06-23	2.3	CVE-2006-3216 MIMESWEEPER BID FRSIRT SECUNIA XF
datetopia -- Dating Agent PRO	requirements.php in Dating Agent PRO 4.7.1 allows remote attackers to obtain sensitive information via a direct request, which calls the phpinfo function.	2006-06-22 2006-06-28	2.3	CVE-2006-3282 BUGTRAQ FRSIRT SECUNIA
datetopia -- Dating Agent PRO	Cross-site scripting (XSS) vulnerability in Dating Agent PRO 4.7.1 allows remote attackers to inject arbitrary web script or HTML via the login parameter in (1) webmaster/index.php and (2) search.php.	2006-06-22 2006-06-28	1.9	CVE-2006-3284 BUGTRAQ FRSIRT SECUNIA XF

dotProject -- dotProject	Cross-site scripting (XSS) vulnerability in classes/ui.class.php in dotProject 2.0.3 and earlier allows remote attackers to inject arbitrary web script or HTML via the login parameter.	unknown 2006-06-27	1.9	CVE-2006-3240 OTHER-REF OTHER-REF OTHER-REF FRSIRT SECUNIA BID
e107.org -- e107 website system	Multiple cross-site scripting (XSS) vulnerabilities in e107 0.7.5 allow remote attackers to inject arbitrary web script or HTML via the (1) ep parameter to search.php and the (2) subject parameter in comment.php (aka the Subject field when posting a comment).	2006-06-18 2006-06-27	2.3	CVE-2006-3259 BUGTRAQ BID FRSIRT SECUNIA
Fortinet -- FortiOS	The FTP proxy module in Fortinet FortiOS (FortiGate) before 2.80 MR12 and 3.0 MR2 allows remote attackers to bypass anti-virus scanning via the Enhanced Passive (EPSV) FTP mode.	unknown 2006-06-24	2.3	CVE-2006-3222 OTHER-REF BID FRSIRT SECUNIA
George Currums -- Open Guestbook	Cross-site scripting (XSS) vulnerability in header.php in Open Guestbook 0.5 allows remote attackers to inject arbitrary web script or HTML via the title parameter.	unknown 2006-06-28	2.3	CVE-2006-3295 BUGTRAQ BID XF
GL-SH -- Deaf Forum	Cross-site scripting (XSS) vulnerability in show.php in GL-SH Deaf Forum 6.4.3 and earlier allows remote attackers to inject arbitrary web script or HTML via the sort parameter.	unknown 2006-06-27	1.9	CVE-2006-3246 OTHER-REF FRSIRT SECUNIA
GL-SH -- Deaf Forum	Multiple cross-site scripting (XSS) vulnerabilities in show.php in GL-SH Deaf Forum 6.4.3 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) search, (2) page, and (3) action parameters. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2006-06-27	1.9	CVE-2006-3247 OTHER-REF FRSIRT SECUNIA
Hitachi -- Groupmax Address Server Hitachi -- Groupmax Mail Server	Unspecified vulnerability in Hitachi Groupmax Address Server 7 and earlier, and Groupmax Mail Server 7 and earlier allows remote attackers to cause a denial of service (product "stop") via unspecified vectors involving "unexpected requests".	unknown 2006-06-23	2.3	CVE-2006-3214 HITACHI FRSIRT SECTRACK SECUNIA XF
IBM -- Websphere Application Server	Unspecified vulnerability in IBM WebSphere Application Server before 6.0.2.11 allows remote attackers to obtain the source code of JSP files via unknown vectors.	unknown 2006-06-27	2.3	CVE-2006-3231 OTHER-REF BID FRSIRT SECUNIA

JaguarSoft -- JaguarEdit	JaguarEditControl (JEdit) ActiveX Control 1.1.0.20 and earlier allows remote attackers to obtain sensitive information, such as the username and MAC and IP addresses, by setting the test field to certain values such as 2404 or 2790, then reading the information from the .JText field.	unknown 2006-06-23	1.9	CVE-2006-3217 BUGTRAQ SRLABS SRLABS BID FRSIRT SECUNIA XF
Jelsoft -- vBulletin	Cross-site scripting (XSS) vulnerability in member.php in vBulletin 3.5.x allows remote attackers to inject arbitrary web script or HTML via the u parameter.	unknown 2006-06-27	1.9	CVE-2006-3253 BUGTRAQ SECTRACK
Jon Link -- Some Chess	Cross-site request forgery (CSRF) vulnerability in menu.php in Some Chess 1.5 rc2 allows remote attackers to conduct actions as another user, such as changing usernames and passwords, via unspecified vectors. NOTE: the provenance of this information is unknown; the details are obtained from third party information.	unknown 2006-06-28	2.3	CVE-2006-3272 SECUNIA
Jon Link -- Some Chess	Cross-site scripting (XSS) vulnerability in menu.php in Some Chess 1.5 rc1 allows remote attackers to inject arbitrary web script or HTML via the user parameter ("New Name" field).	unknown 2006-06-28	1.9	CVE-2006-3273 BUGTRAQ SECTRACK SECUNIA XF
Lanap BotDetect -- CAPTCHA ASP.NET	The Lanap BotDetect APS.NET CAPTCHA component before 1.5.4.0 stores the UUID and hash for a CAPTCHA in the ViewState of a page, which makes it easier for remote attackers to conduct automated attacks by "replaying the ViewState for a known number."	unknown 2006-06-23	2.3	CVE-2006-2918 BUGTRAQ BID OTHER-REF FRSIRT SECUNIA SECTRACK XF
Linux -- Linux kernel	The strnlen_user function in Linux kernel before 2.6.16 on IBM S/390 can return an incorrect value, which allows local users to cause a denial of service via unknown vectors.	unknown 2006-06-27	1.6	CVE-2006-0456 OTHER-REF OTHER-REF OTHER-REF OTHER-REF DEBIAN FRSIRT BID
Linux -- Linux kernel	Linux kernel before 2.6.16.21 and 2.6.17, when running on PowerPC, does not perform certain required access_ok checks, which allows local users to read arbitrary kernel memory on 64-bit systems (signal_64.c) and cause a denial of service (crash) and possibly read kernel memory on 32-bit systems	unknown 2006-06-23	3.7	CVE-2006-2448 OTHER-REF OTHER-REF OTHER-REF BID FRSIRT BUGTRAQ

	(signal_32.c).			TRUSTIX SECUNIA
LookNet -- FineShop	Multiple cross-site scripting (XSS) vulnerabilities in index.php in FineShop 3.0 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) promocja, (2) wysw, or (3) id_produc parameters.	unknown 2006-06-27	1.9	CVE-2006-3235 OTHER-REF SECTRACK XF
MailEnable -- MailEnable	The SMTP service of MailEnable Standard 1.92 and earlier, Professional 2.0 and earlier, and Enterprise 2.0 and earlier before the MESMTPC hotfix, allows remote attackers to cause a denial of service (application crash) via a HELO command with a null byte in the argument, possibly triggering a length inconsistency or a missing argument.	unknown 2006-06-28	2.3	CVE-2006-3277 BUGTRAQ OTHER-REF OTHER-REF BID FRSIRT SECTRACK SECUNIA OTHER-REF XF
MetalheadWs -- Usenet	Cross-site scripting (XSS) vulnerability in index.php in Usenet Script 0.5 allows remote attackers to inject arbitrary web script or HTML via the group parameter.	unknown 2006-06-28	2.3	CVE-2006-3299 BUGTRAQ BID FRSIRT SECUNIA
mvnForum -- mvnForum	Multiple cross-site scripting (XSS) vulnerabilities in activatemember in mvnForum 1.0 GA and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) member and (2) activatecode parameters.	unknown 2006-06-27	1.9	CVE-2006-3245 OTHER-REF SECUNIA BID FRSIRT XF
Namo -- DeepSearch	Cross-site scripting (XSS) vulnerability in mclient.cgi in Namo DeepSearch 4.5 allows remote attackers to inject arbitrary web script or HTML via the p parameter.	2006-06-21 2006-06-27	1.9	CVE-2006-3264 BUGTRAQ OTHER-REF BID FRSIRT SECTRACK SECUNIA XF
Netsoft -- smartNet	Cross-site scripting (XSS) vulnerability in search.jsp in Netsoft smartNet 2.0 allows remote attackers to inject arbitrary web script or HTML via the keyWord parameter.	2006-06-21 2006-06-29	2.3	CVE-2006-3313 BUGTRAQ OTHER-REF BID OTHER-REF SECTRACK XF
New Atlanta Communications -- BlueDragon Server	BlueDragon Server and Server JX 6.2.1.286 for Windows allows remote attackers to cause a dneial of service (hang) via a request	2006-03-09 2006-06-26	2.3	CVE-2006-2310 OTHER-REF FRSIRT

JX New Atlanta Communications -- BlueDragon Server	for a .cfm file whose name contains an MS-DOS device name such as (1) con, (2) aux, (3) com1, and (4) com2.			SECUNIA BID
New Atlanta Communications -- BlueDragon Server JX New Atlanta Communications -- BlueDragon Server	Cross-site scripting (XSS) vulnerability in BlueDragon Server and Server JX 6.2.1.286 for Windows allows remote attackers to inject arbitrary web script or HTML via the filename in a request to a (1) .cfm or (2) .cfml file, which reflects the result in the default error page.	2006-03-09 2006-06-26	1.9	CVE-2006-2311 OTHER-REF FRSIRT SECUNIA
Novell -- Groupwise	Unspecified vulnerability in the Windows Client API in Novell GroupWise 5.x through 7 might allow users to obtain "random programmatic access" to other email within the same post office.	unknown 2006-06-29	2.3	CVE-2006-3268 OTHER-REF OTHER-REF OTHER-REF BID FRSIRT SECUNIA
Open WebMail -- Open WebMail	Cross-site scripting (XSS) vulnerability in OpenWebMail (OWM) 2.52, and other versions released before 05/12/2006, allows remote attackers to inject arbitrary web script or HTML via the (1) To and (2) From fields in openwebmail-main.pl, and possibly (3) other unspecified vectors related to "openwebmailerror calls that need to display HTML."	unknown 2006-06-26	2.3	CVE-2006-3229 OTHER-REF OTHER-REF MLIST
Open WebMail -- Open WebMail	Cross-site scripting (XSS) vulnerability in openwebmail-read.pl in OpenWebMail (OWM) 2.52, and other versions released before 06/18/2006, allows remote attackers to inject arbitrary web script or HTML via the from field. NOTE: some third party sources have mentioned the "to" and "from" fields, although CVE analysis shows that these are associated with the previous version, a different executable, and a different CVE.	unknown 2006-06-27	2.3	CVE-2006-3233 MLIST OTHER-REF OTHER-REF BID
phpQLAdmin -- phpQLAdmin	Multiple cross-site scripting (XSS) vulnerabilities in phpQLAdmin 2.2.7 and earlier allow remote attackers to inject arbitrary web script or HTML via the domain parameter in (1) user_add.php or (2) unit_add.php.	unknown 2006-06-28	2.3	CVE-2006-3301 OTHER-REF BID FRSIRT SECUNIA XF
Positive Software -- H-Sphere	Cross-site scripting (XSS) vulnerability in H-Sphere 2.5.1 Beta 1 and earlier allows remote attackers to inject arbitrary web script or HTML via the (1) next_template, (2) start, (3) curr_menu_id, and (4) arid parameters in	unknown 2006-06-28	1.9	CVE-2006-3278 OTHER-REF FRSIRT SECUNIA

	psoft/servlet/resadmin/psoft.hsphere.C when using the mailman/massmail.html template_name.			
Proton -- EnergyMech IRC Bot	parse_notice (TiCPU) in EnergyMech (emech) before 3.0.2 allows remote attackers to cause a denial of service (crash) via empty IRC CTCP NOTICE messages.	unknown 2006-06-28	2.3	CVE-2006-3293 OTHER-REF GENTOO BID FRSIRT SECUNIA SECUNIA XF
QaTraq -- QaTraq	Multiple cross-site scripting (XSS) vulnerabilities in ashmans and Bill Echlin QaTraq 6.5 RC and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) link_print, (2) link_upgrade, (3) link_sql, (4) link_next, (5) link_prev, and (6) link_list parameters in top.inc as included by queries_view_search.php; the (7) msg, (8) component_name, and (9) component_desc parameters in (a) components_copy_content.php, (b) components_modify_content.php, and (c) components_new_content.php; the (10) title, (11) version, and (12) content parameters in design_copy_content.php; the (13) plan_title and (14) plan_content parameters in design_copy_plan_search.php; the (15) title, (16) minor_version, (17) new_version, and (18) content parameters in design_modify_content.php; the (19) title, (20) version, and (21) content parameters in design_new_content.php; the (22) plan_name and (23) plan_desc parameters in design_new_search.php; the (24) file_name parameter in download.php; the (25) username and (26) password parameters in login.php; the (27) title, (28) version, and (29) content parameters in phase_copy_content.php; the (30) content parameter in phase_delete_search.php; the (31) title, (32) minor_version, (33) new_version, and (34) content parameters in phase_modify_content.php; the (35) content, (36) title, (37) version, and (38) content parameters in phase_modify_search.php; the (39) content parameter in phase_view_search.php; the (40) msg, (41)	unknown 2006-06-29	2.3	CVE-2006-3312 BUGTRAQ OTHER-REF BID

	product_name, and (42) product_desc parameters in products_copy_content.php; and possibly the (43) product_name and (44) product_desc parameters in (d) products_copy_search.php, and a large number of additional parameters and executables.			
Qdig -- Qdig	Multiple cross-site scripting (XSS) vulnerabilities in index.php in Qdig before 1.2.9.3, when register_globals is enabled, allow remote attackers to inject arbitrary web script or HTML via the (1) pre_gallery or (2) post_gallery parameters.	unknown 2006-06-27	1.9	CVE-2006-3265 OTHER-REF FRSIRT SECUNIA
Senokian Solutions -- Enterprise Groupware Systems	Cross-site scripting (XSS) vulnerability in index.php in Enterprise Groupware System (EGS) 1.2.4 and earlier allows remote attackers to inject arbitrary web script or HTML via the module parameter.	unknown 2006-06-27	1.9	CVE-2006-3237 OTHER-REF BID FRSIRT SECTRACK SECUNIA XF
Sun -- ONE Application Server Sun -- Java System Application Server	Cross-site scripting (XSS) vulnerability in Sun ONE Application Server 7 before Update 9, Java System Application Server 7 2004Q2 before Update 5, and Java System Application Server Enterprise Edition 8.1 2005 Q1 allows remote attackers to inject arbitrary HTML or web script via unknown vectors.	unknown 2006-06-26	1.9	CVE-2006-3225 SUNALERT FRSIRT BID SECTRACK SECUNIA XF
Trend Micro -- Control Manager	Cross-site scripting (XSS) vulnerability in Trend Micro Control Manager (TMCM) 3.5 allows remote attackers to inject arbitrary web script or HTML via the username field on the login page, which is not properly sanitized before being displayed in the error log.	unknown 2006-06-27	2.3	CVE-2006-3261 BUGTRAQ BID FRSIRT SECTRACK SECUNIA XF
UebiMiau -- UebiMiau	Multiple cross-site scripting (XSS) vulnerabilities in UebiMiau Webmail 2.7.10, and 2.7.2 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) f_user parameter in index.php, the (2) pag parameter in messages.php, or the (3) lid, (4) tid, and (5) sid parameters in error.php.	unknown 2006-06-28	2.3	CVE-2006-3305 OTHER-REF BID FRSIRT SECUNIA XF
Virtual Design Studios -- vlbook	Cross-site scripting (XSS) vulnerability in index.php in vlbook 1.02 allows remote attackers to inject arbitrary web script or HTML via the message parameter.	unknown 2006-06-27	2.3	CVE-2006-3260 BUGTRAQ ALTERVISTA BID SECUNIA FRSIRT

Webmin -- Webmin	Directory traversal vulnerability in Webmin before 1.280, when run on Windows, allows remote attackers to read arbitrary files via \ (backslash) characters in the URL to certain directories under the web root, such as the image directory.	2006-06-04 2006-06-28	2.3	CVE-2006-3274 BUGTRAQ OTHER-REF OTHER-REF OTHER-REF BID FRSIRT SECTRACK SECUNIA
XennoBB -- XennoBB	Cross-site scripting (XSS) vulnerability in messages.php in XennoBB 1.0.5 and earlier allows remote attackers to inject arbitrary web script or HTML via the tid parameter.	unknown 2006-06-27	1.9	CVE-2006-3241 OTHER-REF FRSIRT SECUNIA
Yahoo -- Yahoo! Messenger	Yahoo! Messenger 7.5.0.814 and 7.0.438 allows remote attackers to cause a denial of service (crash) via messages that contain non-ASCII characters, which triggers the crash in jscript.dll.	unknown 2006-06-28	2.3	CVE-2006-3298 OTHER-REF BID SECUNIA XF
Zoid Technologies -- Project Eros bbsengine	Cross-site scripting (XSS) vulnerability in the preparestring funtion in lib/common.php in Project EROS bbsengine before 20060501-0142-jam, and possibly earlier versions dating back to 2006-02-23, might allow remote attackers to inject arbitrary web script or HTML via unknown vectors.	unknown 2006-06-28	2.3	CVE-2006-3306 OTHER-REF BID FRSIRT SECUNIA XF

Back to top

Last updated July 03, 2006